IN THE CLAIMS:

Please cancel claim 20 without prejudice.

1. (Previously Presented) Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:

an encryption execution unit contained within the pipelined processor;

an ALU contained within the pipelined processor;

an instruction decode stage (ID stage), in response to reading an opcode, enables the encryption execution unit to read data from a memory shared by the ALU and the encryption execution unit, and for the encryption execution unit to process the data read from the shared memory; and

a multiplexer to select as an output a result of processing by the encryption execution unit rather than a result of ALU processing.

2. (Original) The apparatus of Claim 1 wherein the encryption execution unit is an encryption tightly coupled state machine (TCSM) unit that is selectively invoked within the pipelined processor.

3. (Previously Presented) The apparatus of Claim 2, further comprising:

native encryption opcodes provided within an instruction set of the pipelined processor to enable selective access to the encryption TCSM unit by software.

4. (Previously Presented) The apparatus of Claim 3, further comprising:

a plurality of busses internal to the pipelined processor and wherein a hardware portion of the interface allows the encryption TCSM unit to utilize the internal buses in response to decode processing of the native encryption opcodes.

5. (Previously Presented) The apparatus of Claim 4, further comprising:

the pipelined processor is a microcontroller core (TMC) processor having a multi-stage pipeline architecture that includes an instruction fetch stage, an instruction decode stage, an execution stage and a memory write-back stage.

6. (Previously Presented) The apparatus of Claim 5, further comprising:

the TMC processor further includes an arithmetic logic unit, at least one internal register, an instruction fetch and decode unit and the encryption TCSM unit organized as a data path.

7. (Previously Presented) The apparatus of Claim 5 wherein the encryption TCSM unit comprises:

a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

8. (Previously Presented) The apparatus of Claim 7 wherein the DES functional component comprises:

state machine hardware used to execute each round of a DES function.

9. (Previously Presented) The apparatus of Claim 7, further comprising:

the sub-key generation functional component comprises state machine hardware that generates a sub-key as needed for each round of a DES function.

10. (Previously Presented) A method for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the method comprising the steps of:

providing an encryption execution unit within the pipelined processor;

providing an ALU within the pipelined processor;

enabling, by an instruction decode stage (ID stage) in response to reading an op-code, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and

selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

11. (Previously Presented) The method of Claim 10, further comprising:

having native encryption opcodes contained within an instruction set of the pipelined processor; and

issuing the native encryption opcodes directly to the encryption execution unit to substantially reduce encryption setup latency.

12. (Previously Presented) The method of Claim 11, further comprising:

decoding the native encryption opcodes at the instruction decode stage; and

in response to the step of decoding, invoking the encryption execution unit to perform encryption/decryption functions at the execution stage.

13. (Previously Presented) The method of Claim 12, further comprising:

protocol processing of protocols contained in a plaintext stored at the network switch to determine an appropriate encryption algorithm;

upon determining the appropriate encryption algorithm, immediately starting an operation to fetch initial keys needed to perform the encryption/decryption functions; and upon fetching the keys, providing the keys to the encryption execution unit within the TMC processor.

14. (Previously Presented) The method of Claim 13, further comprising:

including a plurality of high-performance busses internal to the TMC processor; and

accessing the internal busses to simultaneously load an encryption key and store a previous encryption result.

15. (Previously Presented) The method of Claim 12 further comprising the step of, wherein the encryption execution unit is an encryption tightly coupled state machine (TCSM) unit:

initializing the encryption TCSM unit in response to execution of a first instruction that defines the form of operation to be performed.

16. (Original) The method of Claim 15 wherein the encryption TCSM unit comprises a data encryption standard (DES) functional component cooperatively coupled to a sub-key

generation functional component and wherein the step of initializing comprises the steps of:

decoding a first portion of the first instruction to initialize the DES functional component; and

decoding a second portion of the first instruction to initialize the sub-key generation functional component.

17. (Original) The method of Claim 16 further comprising the step of:

executing a second instruction having a micro-opcode field containing a native encryption opcode that specifies loading an initial key from a memory into the sub-key generation functional component of the encryption TCSM unit.

18. (Previously Presented) The method of Claim 17 further comprising the step of:

performing a DES function on a plaintext in response to execution of a third instruction having a micro-opcode field containing a native encryption code that specifies loading of the plaintext into the DES functional component of the encryption TCSM unit and initiating DES operations; and

upon completing the DES operations, storing a ciphertext result in an internal register coupled to the DES functional component.

19. (Original) The method of Claim 18 further comprising the step of:

executing a fourth instruction to store the ciphertext results contained in the internal register to a location in the memory.

20. (Canceled)

21. (Previously Presented) A pipelined processor in a network switch, the processor comprising:

an ALU internal to the processor responsive to a first set of opcodes;

an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM) responsive to a second set of opcodes;

an instruction decode stage (ID stage) to decode an opcode, the ID stage, in response to an opcode of said second set of opcodes, transferring processing to the encryption execution unit;

a multiplexer to select output from the ALU OR from the encryption execution unit.

22. (Previously Presented) The processor of Claim 21, wherein the processor is a microcontroller core (TMC) processor and further comprises:

an instruction fetch stage;

an execution stage to execute an instruction decoded by the ID stage; and

a memory write-back stage to write a result of said execution stage to memory.

23. (Previously Presented) The processor of Claim 21, further comprises:

one or more internal registers;

a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit; and

a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

24. (Previously Presented) The processor of Claim 21, wherein the encryption TCSM unit comprises:

a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

25. (Previously Presented) The processor of Claim 24, wherein the DES functional component comprises:

a state machine that executes each round of a DES function.

26. (Previously Presented) The processor of Claim 24, wherein the sub-key generation functional component comprises:

a state machine that generates a sub-key as needed for each round of a DES function.

27. (Previously Presented) A method for providing encryption functions within a pipelined processor in a network switch, the method comprising the steps of:

associating a first set of opcodes with an ALU internal to the processor, the ALU performing protocol processing operations;

associating a second set of opcodes with an encryption execution unit internal to the processor, the encryption execution unit performing encryption operations;

decoding opcodes by an instruction decode stage (ID stage);

transferring by the ID stage, in response to an opcode from said first set of opcodes, processing to the ALU;

transferring by the ID stage, in response to an opcode from said second set of opcodes, processing to the encryption execution unit; and

selecting output from the ALU OR from the encryption execution unit.

28. (Previously Presented) The method of Claim 27, further comprises the step of:

providing one or more internal registers;

providing a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit;

providing a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

29. (Previously Presented) The method of Claim 27 further comprising the step of:

initializing the encryption TCSM unit in response to a first instruction that defines a form of operation to be performed.

30. (Previously Presented) The method of Claim 29, wherein the step of initializing comprises the steps of:

decoding a first portion of the first instruction to initialize a DES functional component; and

decoding a second portion of the first instruction to initialize a sub-key generation functional component.

31. (Previously Presented) The method of Claim 27, further comprising the steps of:

executing a second instruction including an encryption opcode that specifies loading an initial key from a memory into a sub-key generation functional component of the TCSM unit.

32. (Previously Presented) The method of Claim 27, further comprising the steps of:

performing a DES function in response to execution of a third instruction having a field containing an encryption opcode that specifies loading plaintext and initializing a DES operation.

33. (Previously Presented) A computer readable media, comprising:

said computer readable media containing instructions for execution in a processor for the practice of the method of,

providing a tightly-coupling hardware data encryption function with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch;

providing an encryption execution unit within the pipelined processor;

providing an ALU within the pipelined processor;

enabling, by an instruction decode stage (ID stage) in response to reading an op-code, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and

selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

34. (Previously Presented) Electromagnetic signals propagating on a computer network, comprising:

said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of,

providing a tightly-coupling hardware data encryption function with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch;

providing an encryption execution unit within the pipelined processor;

providing an ALU within the pipelined processor;

enabling, by an instruction decode stage (ID stage) in response to reading an opcode, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and

selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

35. (Previously Presented) A router, comprising:

a processor having an instruction decode stage (ID stage) for processing opcodes;

an ALU for performing protocol processing operations;

a tightly coupled state machine (TCSM) for performing encryption processing;

a shared memory for providing data to either the ALU or the TCSM;

the ID stage, in response to reading an opcode, transferring processing to the TCSM, and the TCSM performing encryption processing on data read from the shared memory;

a selector to select as output results from the ALU OR results from the TCSM.

36. (Previously Presented) The apparatus of Claim 35, further comprising:

the selector is a multiplexer.

37. (Previously Presented) The apparatus of Claim 35, further comprising;

the ALU selects whether the ALU or the TCSM reads data from the memory.

38. (Previously Presented) The apparatus of Claim 35, further comprising:

the TCSM performs DES data encryption standard encryption processing.

39. (Previously Presented) The apparatus of Claim 35, further comprising:

a sub-key generation component to provide a key to the TCSM.

40. (Previously Presented) A method for operating a router, comprising:

processing opcodes by an instruction decode stage (ID stage);

performing encryption processing by a tightly coupled state machine (TCSM);

performing protocol processing by an ALU;

reading data from a shared memory by either the ALU or the TCSM;

transferring processing by the ID stage, in response to reading an opcode to the TCSM, and the TCSM performing encryption processing on data read from the shared memory;

selecting as output results from the ALU OR results from the TCSM.

41. (Previously Presented) The method of Claim 40, further comprising:

using a multiplexer for selecting as output results from the ALU OR results from the TCSM.

42. (Previously Presented) The method of Claim 40, further comprising;

selecting whether the ALU or the TCSM reads data from the memory.

43. (Previously Presented) The method of Claim 40, further comprising:

performing DES data encryption standard encryption processing by the TCSM.

44. (Previously Presented) The method of Claim 40, further comprising:

providing a key to the TCSM by a sub-key generation component.

45. (Previously Presented) A router, comprising:

means for providing a processor having an ALU for processing opcodes and a tightly coupled state machine (TCSM) for performing encryption processing;

means for reading data from a shared memory by either the ALU or the TCSM;

means for transferring processing by an instruction decode stage (ID stage), in response to reading an opcode, to the TCSM, and the TCSM performing encryption processing on data read from the shared memory;

means for selecting as output results from the ALU OR results from the TCSM.

46. (Previously Presented) The apparatus of Claim 45, further comprising:

means for using a multiplexer for selecting as output results from the ALU OR results from the TCSM.

47. (Previously Presented) The apparatus of Claim 45, further comprising;

means for selecting by the ALU whether the ALU or the TCSM reads data from the memory.

48. (Previously Presented) The apparatus of Claim 45, further comprising:

means for performing DES data encryption standard encryption processing by the TCSM.

49. (Previously Presented) The apparatus of Claim 45, further comprising:

means for providing a key to the TCSM by a sub-key generation component.

50. (Previously Presented) A computer readable media, comprising:

said computer readable media containing instructions for execution in a processor for the practice of the method of,

providing encryption functions within a pipelined processor in a network switch, having the steps,

associating a first set of opcodes with an ALU internal to the processor, the ALU performing protocol processing operations;

associating a second set of opcodes with an encryption execution unit internal to the processor, the encryption execution unit performing encryption operations;

decoding opcodes by an instruction decode stage (ID stage);

transferring by the ID stage, in response to an opcode from the first set of opcodes, processing to the ALU;

transferring by the ID stage, in response to an opcode from said second set of opcodes, processing to the encryption execution unit; and

selecting output from the ALU OR from the encryption execution unit.

51. (Previously Presented) Electromagnetic signals propagating on a computer network, comprising:

said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of,

providing encryption functions within a pipelined processor in a network switch, having the steps,

associating a first set of opcodes with an ALU internal to the processor, the ALU performing protocol processing operations;

associating a second set of opcodes with an encryption execution unit internal to the processor, the encryption execution unit performing encryption operations;

decoding opcodes by an instruction decode stage (ID stage);

transferring by the ID stage, in response to an opcode from the first set of opcodes, processing to the ALU;

transferring by the ID stage, in response to an opcode from said second set of opcodes, processing to the encryption execution unit; and

selecting output from the ALU OR from the encryption execution unit.

52. (Previously Presented) A computer readable media, comprising:

said computer readable media containing instructions for execution in a processor for the practice of the method of operating a router, having the steps,

processing opcodes by an instruction decode stage (ID stage);

performing encryption processing by a tightly coupled state machine (TCSM);

performing protocol processing by an ALU;

reading data from a shared memory by either the ALU or the TCSM;

transferring processing by the ID stage, in response to reading an opcode to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; and

electing as output results from the ALU OR results from the TCSM.

53. (Previously Presented) Electromagnetic signals propagating on a computer network, comprising:

said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of operating a router, having the steps, processing opcodes by an instruction decode stage (ID stage);

performing encryption processing by a tightly coupled state machine (TCSM);

performing protocol processing by an ALU;

reading data from a shared memory by either the ALU or the TCSM;

transferring processing by the ID stage, in response to reading an opcode to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; and

selecting as output results from the ALU OR results from the TCSM.